Safeguard Computer Security Evaluation Matrix (SCSEM)

Management, Operational and Technical Controls

Release IV

7-Dec-07

Internal
Revenue
Service

Tester: *Insert Tester Name*
Date: *Insert Date(s) Testing Occured*
Location: *Insert Location testing was conducted*
Agency POC(s): *Insert Agency interviewee(s) names*

ID	PUB 1075			Control Objective	Test Procedure & Expected Results	Pass / Fail	Actual Results	Comments / Supporting Evidence
	Control Class	Control Family	REF. ID					
1	M	RA	RA-1	Risk Assessment Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	Procedures: 1. Examine risk assessment policy and procedures. 2. Interview agency personnel with risk assessment responsibilities to determine how often risk assessment policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine risk assessment policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. Risk assessment policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the Agency. 2. Risk assessment policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when Agency review indicates updates are required. 3. Risk assessment policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.			

2	M	RA	RA-2	Security Categorization: The Agency categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the Agency review and approve the security categorizations	Procedures: 1. Examine the system security categorization. Expected Results: 1. The results of the security categorization are documented and are consistent with FIPS-199 and NIST SP 800-60 methodology. 2. The security categorization includes supporting rationale for impact-level decisions. 3. Senior level agency official has reviewed and approved the security categorization.			
	M	RA	RA-3	Risk Assessment: The Agency conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).	Procedures: 1. Examine the most recent risk assessment conducted on the system. 2. Examine risk assessment and verify it was performed in accordance with applicable guidance. Expected Results: 1. Risk assessment has been conducted and documented that includes the magnitude of harm that could result from the unauthorized access, use, disclosure, modification, or destruction of the information and the information systems that support its operations and assets (including information and information systems managed/operated by external parties). 2. The risk assessment is consistent with NIST SP 800-30 methodology.			

3	M	RA	RA-3	Risk Assessment Update: The Agency updates the risk assessment at a minimum of three years or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.	Procedures: 1. Examine risk assessment policy and procedures to determine how often risk assessments are updated. 2. Examine the most recent risk assessment conducted on the system and interview personnel with risk assessment responsibility to determine if the report reflects the latest significant changes. Expected Results: 1. The risk assessment is updated at a minimum of three years or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security status of the system. 2. The risk assessment was performed within the last three years and reflects the latest significant changes to the information system, the facilities where the system resides, or other conditions that may have impacted the security status of the system..			
4	M	RA	RA-5	Vulnerability Scanning: The Agency conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).	Procedures: 1. Examine risk assessment policy and procedure and interview personnel with risk assessment responsibility to determine how often the system is scanned for vulnerabilities. 2. Examine the latest vulnerability scanning results report. 3. Examine the scanning tool used by the agency to verify its functionality. Expected Results: 1. The agency scans the information system for vulnerabilities quarterly or when significant new vulnerabilities are identified and reported. 2. The vulnerability scan was conducted within the last quarter, or more recently. 3. The agency uses scanning tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact.			

5	M	PL	PL-1	Security Planning Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	Procedures: 1. Examine security planning policy and procedures. 2. Interview Agency personnel with security planning responsibilities to determine how often security planning policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine security planning policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. Security planning policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the agency. 2. Security planning policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Security planning policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.			
6	M	PL	PL-2	System Security Plan: The Agency develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan	Procedures: 1. Examine the most recent system security plan. Expected Results: 1. The security plan provides an overview of the security requirements for the information system and a description of the security controls planned or in place for meeting the security requirements. The security plan was developed in accordance with NIST SP 800-18 methodology. 2. Designated agency officials have reviewed and approved the security plan.			

7	M	PL	PL-3	System Security Plan Update: The Agency reviews the security plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.	Procedures: 1. Examine security planning policy and procedures to determine how often the security plan is reviewed and updated. Expected Results: 1. The system security plan is reviewed annually. During reviews, major changes to the agency, information system and problems with security plan implementation and security control enhancements are considered for updates.			
8	M	PL	PL-4	Rules Of Behavior: The Agency establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information system usage. The Agency receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.	Procedures: 1. Examine the system's Rules of Behavior. 2. Interview an authorized system user to determine their awareness of the rules of behavior. 3. Examine user's signed Rules of Behavior document. Expected Results: 1. The Rules of Behavior establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage. 2. The user is aware of the Rules of Behavior, and the document is readily available to them. 3. The Rules of Behavior document is signed, indicating acknowledgement from the user that they have read, understand, and agree to abide by the rules of behavior.			

9		PL	PL-6	Security-Related Activity Planning: The Agency plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on Agency operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.	Procedures: 1. Examine security planning policy and procedures and interview personnel with security planning responsibility to determine if system security related activities are properly coordinated. Expected Results: 1. Security-related activities including, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises are coordinated prior to execution to limit the impact on agency operations.			
10	M	SA	SA-1	System And Services Acquisition Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	Procedures: 1. Examine system services and acquisition policy and procedures. 2. Interview agency personnel with system services and acquisition responsibilities to determine how often system services and acquisition policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine system services and acquisition policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. System services and acquisition policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the agency. 2. System services and acquisition policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. System services and acquisition policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.			

11	M	SA	SA-2	Allocation of Resources: The Agency determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system	Procedures: 1. Examine system services and acquisition policy and interview agency personnel with services and acquisition responsibility to determine how resources are allocated for system security requirements/mechanisms. 2. Examine information system business case planning and budgeting documentation. Expected Results: 1. The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system; 2. The organization determines security requirements for the information system in mission/business case planning. A discrete line item for information system security is established in the organization’s programming and budgeting documentation.			
12	M	SA	SA-3	Life Cycle Support: The Agency manages the information system using a system development life cycle methodology that includes information security considerations	Procedures: 1. Examine information system development life cycle documentation. 2. Examine the agency's system development life cycle. Expected Results: 1. The agency manages the system using a system development life cycle methodology that includes information security considerations. 2. The agency uses a system development life cycle that is consistent with NIST Special Publication 800-64 by including the following phases: initiation, acquisition/development, implementation, operations/maintenance, and disposition. Each of these five phases includes a minimum set of security steps to effectively incorporate security into a system during its development. **Note:** The agency will either use the general SDLC described in the expected result or will have developed a tailored SDLC that meets their specific needs. In either case, security steps shall be incorporated into the agency's SDLC.			

13	M	SA	SA-4	Acquisitions: The Agency includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	Procedures: 1. Examine system acquisition documentation, including acquisition contracts for the information system or services. 2. Examine system acquisition documentation to determine if guidance is provided on the acquisition and use of tested/evaluated information technology products. Expected Results: 1. Acquisition contracts for information systems include, either explicitly or by reference, security requirements and/or security specifications that describe: -required security capabilities; -required design and development processes; -required test and evaluation procedures; and -required documentation. 2. To be consistent with NIST 800-23, the agency gives substantial consideration to procuring commercial IT products that have been evaluated and tested by independent accredited laboratories against appropriate security specifications and requirements.			
14	M	SA	SA-5	Information System Documentation: The Agency obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. (The Agency ensures that adequate documentation for the information system is available, protected when required, and distributed to authorized personnel).	Procedures: 1. Examine information system documentation, including administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system’s security features. 2. Interview personnel operating, using or maintaining the system to verify information system documentation is made available. 3. Examine the location of information system documentation, either in hard copy or soft copy. Expected Results: 1. Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system’s security features. 2. Operational personnel has knowledge of, and an available copy of the documentation. 3. Information system documentation is made available to authorized personnel only.			

15	M	SA	SA-6	Software Usage Restrictions: The Agency complies with software usage restrictions.	Procedures: 1 & 2. Examine the list of software usage restrictions. 3. Examine inventory of licensed software installed on the system, and site software license documentation. Expected Results: 1. The policy mandates a regular review of software usage for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. 2. The policy controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. 3. Only licensed and approved software is contained in the inventory of software installed on the system. The agency makes use of a controlled implementation process for licensed software and employs tracking systems to control copying and distribution.			
16	M	SA	SA-7	User Installed Software: The Agency enforces explicit rules governing the installation of software by users.	Procedures: 1. Examine software usage restriction policy and/or list of rules governing user installed software. Expected Results: 1. The agency enforces explicit rules governing the installation of software by users. The policy identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is free only for personal, not government use, and is potentially malicious). The agency regularly reviews/analyzes user installed software for indications of inappropriate or unusual activity,			

17	M	SA	SA-8	Security Engineering Principles: The Agency designs and implements the information system using security engineering principles.	Procedures: 1. Examine information system design documentation, security requirements and security specifications for the security design principles used for new information systems and for system upgrades and modifications. Expected Results: 1. The agency designs and implements the information system using security engineering principles consistent with NIST SP 800-27, e.g., establish a sound security policy as the foundation of design, ensure developers are trained in how to develop secure software, implement layered security. See NIST 800-27 for a complete list of the security engineering principles. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.			
18	M	SA	SA-9	External Information System Services: The Agency: (i) requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.	Procedures: 1. Interview agency personnel to determine if information system services for systems that store, process or transmit FTI are implemented by a provider external to the agency. 2. Interview agency personnel to determine if the agency monitors security control compliance of external information system providers. Expected Results: 1. If information system services are implemented by an external provider, the agency requires that providers of external information system services employ adequate security controls, including how FTI is handled and protected at the external site, including any information stored, processed, or transmitted using the provider's computer systems; the background investigation and/or clearances requirements for external providers with access to FTI, and security awareness and training requirements for external providers with access to FTI. 2. The agency regularly reviews/analyzes external providers of information system services for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions;			

19	M	SA	SA-11	Developer Security Testing: The Agency requires that information system developers create a security test and evaluation plan, implement the plan, and document the results.	Procedures: 1. Interview agency personnel to determine if security test and evaluations are performed during system development. 2. Examine security test and evaluation plan and results from system development, or the most recent modification to the system. Expected Results: 1. The agency requires that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results for newly developed systems and modifications to existing systems that impact security controls. 2. Security test and evaluation plan and results are available and document the test cases executed and results of each test.			

20	M	CA	CA-1	Certification, Accreditation, And Security Assessment Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.	Procedures: 1. Examine Certification, Accreditation, And Security Assessment policy and procedures. 2. Interview agency personnel with Certification, Accreditation, And Security Assessment responsibilities to determine how often Certification, Accreditation, And Security Assessment policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine Certification, Accreditation, And Security Assessment policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. Certification, Accreditation, And Security Assessment policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the agency. 2. Certification, Accreditation, And Security Assessment policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Certification, Accreditation, And Security Assessment policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.			

21	M	CA	CA-2	Security Assessments: The Agency conducts an assessment of the security controls in the information system at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	Procedures: 1. Examine the results from the last security control assessment and determine whether the agency conducts security assessments annually, or when a major change occurs. 2. Examine the results from the last security control assessment to determine if the security controls are assessed for correct implementation, for intended operation, and for producing the desired outcome with respect to meeting the security requirements for the system. Expected Results: 1. The results from the last security control assessment are available and an assessment of the security controls in the information system is conducted annually, or when a major change occurs. 2. Security controls are assessed for correct implementation and meet the security requirements for the system.			
22	M	CA	CA-3	Information System Connections: The Agency authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis	Procedures: 1. Examine a list of all connections connected to the information system outside of its boundary. 2. Examine MOUs/ISAs to determine if the agreements are consistent with NIST Special Publication 800-47. Expected Results: 1. The information system has all required MOUs/ISAs for all connections external to the system boundary. 2. The agency authorizes all connections from the information system to external information systems through the use of system connection agreements; and MOUs/ISAs are consistent with NIST Special Publication 800-47 by including: Interconnection statement of requirements which addresses the requirement for the interconnection, the names of the systems being connected and the agency that initiated the inteconnection; System security considerations, including a topological diagram and a signature line for the DAA of each system to sign. See NIST 800-47 for more detailed information and a sample template.			

23	M	CA	CA-4	Security Certification: The Agency conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	Procedures: 1. Examine the most recent security assessment plan, results and report. 2. Examine procedures addressing security certification to determine if the agency employs a security certification process in accordance with NIST SP 800-37 and 800-53A. Expected Results: 1. The agency conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. 2. The agency employs security certification process in accordance with NIST SP 800-37 and the assessment procedures provied in NIST SP 800-53A. The agency assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the agency assesses a subset of the controls annually during continuous monitoring.			
24	M	CA	CA-5	Plan Of Action And Milestones: The Agency develops and updates quarterly, a plan of action and milestones for the information system that documents the Agency’s planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.	Procedures: 1. Examine the plan of action and milestones (POA&M) corresponding to the last security control assessment. Expected Results: 1. The POA&M documents the planned, implemented, and evaluated actions to correct the deficiencies and vulnerabilities in the system identified from audits, assessments, and known vulnerabilities, and was updated with results from the most recent security control assessment.			

25	M	CA	CA-6	Security Accreditation: The Agency authorizes (i.e., accredits) the information system for processing before operations and updates the authorization at least every three years or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation	Procedures: 1. Examine the security accreditation documentation. 2. Examine agency security accreditation policy to verify policy for conducting accreditation when there is a major system change. Expected Results: 1. The accreditation documentation contains the accreditation memo, or equivalent document signed by the system DAA authorizing the system for processing. 2. The agency updates the authorization when there is a significant change to the information system.			

26	M	CA	CA-7	Continuous Monitoring: The Agency monitors the security controls in the information system on an ongoing basis.	Procedures: 1. Examine policy and procedures addressing continuous monitoring of system security controls. 2. Examine policy and procedures addressing continuous monitoring of system security controls, examine security impact analyses. 3. Examine policy and procedures addressing continuous monitoring of system security controls Expected Results: 1. Continuous monitoring policy and procedures address configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. the organization assesses a subset of the controls annually during continuous monitoring. 2. The agency conducts security impact analyses on changes to the information system; the agency documents and reports changes to the security controls employed in the system and updates the system security plan and POA&M as appropriate based on outcome of continuous monitoring activities. 3. The policy establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system for assessment based on FIPS 199 security categorization.			

27	O	PS	PS-1	Personnel Security Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	Procedures: 1. Examine personnel security policy and procedures. 2. Interview agency personnel with personnel security responsibilities to determine how often personnel security policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine personnel security policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. Personnel security policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the Agency. 2. Personnel security policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when Agency review indicates updates are required. 3. Personnel security policy should address the following areas: Position Categorization, Personnel Screening, Personnel Termination, Personnel Transfer, and Access Agreements. Personnel security policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.			
28	O	PS	PS-2	Position Categorization: The Agency assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The Agency reviews and revises position risk designations as defined in the agency personnel security policy.	Procedures: 1. Examine a list of risk designations for agency positions that require access to FTI. 2. Examine the personnel security policy to verify the screening criteria. 3. Examine the personnel security policy to verify the frequency that position descriptions are reviewed and updated. Expected Results: 1. The agency assigns a risk designation to all positions requiring access to FTI. 2. The agency establishes a screening criteria for individuals filling organizational positions requiring access to FTI. 3. The agency reviews and revises position risk designations in accordance with the agency personnel security policy.			

29	O	PS	PS-3	Personnel Screening: The Agency screens individuals requiring access to Agency information and information systems before authorizing access.	Procedures: 1. Examine applicable documents to determine if the Agency appropriately screens individuals requiring access to Agency information and information systems prior to authorizing access. 2. Examine a sample of the personnel records to verify that each employee was subject to background screening in accordance with agency personnel policy before being granted information system access. Sample Size = 5 Expected Results: 1. The agency screens individuals requiring access to agency information systems containing FTI prior to authorizing access. 2. Each of the new employees was subject to the appropriate background screening before they were granted information system access. At least an interim clearance was obtained before being granted information system access. Note: As it can take up to one year for a background investigation to be completed. As long as the background investigation is on-going (i.e., a proof of investigation exists), this test case should pass.			
30	O	PS	PS-4	Personnel Termination: When employment is terminated, the Agency terminates information system access, conducts exit interviews, ensures the return of all Agency information system-related property (e.g., keys, identification cards, building passes), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on Agency information systems.	Procedures: 1. Examine agency employee termination procedures and interview agency employees with personnel security responsibility. 2. Examine a list of recently terminated employees and verify that records of personnel termination exist for those employees. Sample Size =5 (if available) Expected Results: 1. The agency terminates information system access upon termination of individual employment, conducts exit interviews of terminated personnel, retrieves all organizational information system-related property, e.g., keys, identification cards, and building passes from terminated personnel, and retains access to official documents and records on organizational information systems created by terminated personnel. 2. All terminated employees on the list have an associated record of termination activities performed in accordance with agency policy.			

31	O	PS	PS-5	Personnel Transfer: The Agency reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the Agency and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).	Procedures: 1. Examine agency employee transfer procedures and interview agency employees with personnel security responsibility.. 2. Examine a list of recently transferred employees and verify that records of personnel transfer exist for those employees. Sample Size = 5 (if available) Expected Results: 1. The agency (i) reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the Agency; and (ii) initiates the following appropriate actions: reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization for personnel reassigned or transferred within the organization. 2. All transferred employees on the list have an associated record of transfer activities performed in accordance with agency policy.			
32	O	PS	PS-6	Access Agreements: The Agency must complete appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals before authorizing access to Federal tax information and information systems providing access to such information.	Procedures: 1. Examine a list of employee access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for current employees who have access to systems containing FTI. Sample Size = 5 Expected Results: 1. Employees access agreements are signed before being authorized access to systems containing FTI.			

33	O	PS	PS-7	Third Party Personnel Security: The Agency establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.	Procedures: 1. Interview agency personnel to determine if third-party providers (e.g., third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.) are utilized by the agency for systems containing FTI. 2. Examine acquisition related documents (e.g, contracts, service level agreements) for the third party provider to verify personnel security requirements are included. 3. Interview agency personnel with personnel security responsibility and examine compliance reports to verify techniques for monitoring compliance with personnel security requirements. Expected Results: 1. If no third party providers are utilized, this control can be marked N/A. If third party providers are utilized, proceed to test procedure number 2. 2. Acquistion related documents contain requirements for the third party provider to ensure they must follow agency personnel security requirements. 3. The agency uses mechanisms such as compliance reports to ensure the third party provider complies with agency personnel security requirements.			
34	O	PS	PS-8	Personnel Sanctions: The Agency employs a formal sanctions process for personnel failing to comply with established information security policies and procedures	Procedures: 1. Examine personnel security policy and information system rules of behavior documents. Expected Results: 1. The policy and rules of behavior documents contain a formal sanctions process for personnel failing to comply with agency information security policies and procedures.			

35	O	CP	CP-1	Contingency Planning Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	Procedures: 1. Examine contingency planning policy and procedures. 2. Interview agency personnel with contingency planning responsibilities to determine how often contingency planning policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine contingency planning policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. Contingency planning policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the Agency. 2. Contingency planning policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when Agency review indicates updates are required. 3. Contingency planning policy should address the following areas: Alternate Storage Sites, Telecommunication Services, and Information System Backup.			

36	O	CP	CP-2	Contingency Plan: The Agency develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.	Procedures: 1. Examine the IT Contingency Plan (ITCP) for the information system(s) processing, storing or transmitting FTI. 2. Examine procedures addressing contingency operations for the information system(s). Expected Results: 1. The ITCP addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system consistent with NIST Special Publication 800-34. 2. The contingency plan is reviewed and approved by designated organizational officials, and disseminated to key personnel with contingency planning responsibility.			

37	O	CP	CP-4	Contingency Plan Testing and Exercises: The Agency: (i) tests and/or exercises the contingency plan for the information system [Assignment: Agency-defined frequency, at least annually] using [Assignment: Agency-defined tests and/or exercises] to determine the plan's effectiveness and the Agency's readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions.	Procedures: 1. Examine contingency plan testing and/or exercise documentation. 2. Examine contingency plan testing records documents the results of contingency plan testing/exercises. Expected Results: 1. The agency defines the set of contingency plan tests and/or exercises, and tests/exercises the contingency plan annually. 2. Testing records document the results of contingency plan testing/exercises.			
38	O	CP	CP-5	Contingency Plan Update: The Agency reviews the contingency plan for the information system [Assignment: Agency-defined frequency, at least annually] and revises the plan to address system/Agency changes or problems encountered during plan implementation, execution, or testing.	Procedures: 1. Examine contingency planning policy to determine ITCP update schedule. Expected Results: 1. The agency updates the contingency plan at least annually based on experiences during plan implementation, execution, and testing.			

39	O	CP	CP-6	Alternate Storage Sites: The Agency identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.	Procedures: 1. Examine procedures addressing alternate storage sites, or interview personnel with alternate storage site responsibility. 2. Examine alternate storage site agreements. Expected Results: 1. The agency identifies an alternate storage site; 2. The alternate storage site agreements are currently in place, available, accessible, and meets the requirements (including necessary equipment and supplies) to permit the storage of information system backup.			
40	O	CP	CP-7	Alternate Processing Sites: The Agency identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [Assignment: Agency-defined time period] when the primary processing capabilities are unavailable.	Procedures: 1. Examine procedures addressing alternate processing sites, or interview personnel with alternate processing site responsibility. 2. Examine alternate processing site agreements. Expected Results: 1. The agency identifies an alternate processing site. 2. Alternate processing site agreements are currently in place to permit the resumption of information system operations for critical mission/business functions, and defines the time period within which processing must be resumed at the alternate processing site.			

41	O	CM	CM-1	Configuration Management Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	Procedures: 1. Examine configuration management policy and procedures. 2. Interview agency personnel with configuration management responsibilities to determine how often configuration management policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine configuration management policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. Configuration management policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the Agency. 2. Configuration management policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when Agency review indicates updates are required. 3. Configuration management policy should address the following areas: Alternate Storage Sites, Telecommunication Services, and Information System Backup.			
42	O	CM	CM-2	Baseline Configuration: The Agency develops, documents, and maintains a current baseline configuration of the information system	Procedures: 1/2. Examine the information system baseline configuration. Expected Results: 1. The agency maintains a documented baseline configuration of the information system that provides the organization with a well-defined and documented specification to which the information system is built (e.g., software versions, patch level) 2. The baseline configuration includes documented deviations from the baseline configuration.			

43	O	CM	CM-3	Configuration Change Control: The organization authorizes, documents, and controls changes to the information system.	Procedures: 1. Examine configuration management policy and procedures and agency configuration management plan. 2. Examine change request documentation for specific information systems changes. Expected Results: 1. The agency manages configuration changes to the information system using an organizationally approved process (e.g., a chartered Configuration Control Board) that includes an approval process for emergency changes. 2. The change request documentation shows that the agency authorizes, documents, and controls changes to the information system.			
44	O	CM	CM-4	Monitoring Configuration Changes: The Agency monitors changes to the information system conducting security impact analyses to determine the effects of the changes.	Procedures: 1. Examine change request documentation for specific system changes. Expected Results: 1. The change request documentation includes an analysis for potential security impacts, and after the change is implemented, (including upgrades and modifications), the functionality of the security features are verified to still be functioning properly.			
45	O	CM	CM-5	Access Restrictions For Change: The Agency: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes.	Procedures: 1/2. Examine the list of personnel authorized access to the information system for the purpose of initiating changes. Expected Results: 1. The agency maintains a list of qualified and authorized personnel permitted to access the information system for the express purpose of initiating changes. the ability to make configuration changes is restricted to authorized development and configuration management staff only and list of the staff is maintained. No system administrator, database administrator or end user has the ability to make configuration changes. 2. The agency generates, retains, and reviews records reflecting all such changes to the information system..			

45	O	CM	CM-6	Configuration Settings: The Agency: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with information system operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.	Procedures: 1. Examine configuration management policy. 2. Examine platform specific secure configuration guidance to determine if system configurations follow configuration management policy. 3. Examine technical control SCSEM results for each technical platform within scope from the Safeguard review. Expected Results: 1. The agency establishes and documents mandatory configuration settings for information technology products employed within the information system. 2. The agency configures the security settings of information technology products to the most restrictive mode consistent with operational requirements. 3. Results from the technical control SCSEMs indicate systems are configured in compliance with agency configuration settings policy.			
47	O	CM	CM-7	Least Functionality: The Agency must configure the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of unnecessary functions, ports, protocols, or services	Procedures: 1. Examine configuration management policy and platform specific secure configuration guidance. 2. Examine technical control SCSEM results for each technical platform within scope from the Safeguard review. Expected Procedures: 1. The agency identifies prohibited or restricted functions, ports, protocols, and services for the information system. 2. Results from the technical control SCSEMs indicate the systems are configured to provide only essential capabilities and restrict the functions, ports, protocols and services prohibited by policy.			

48	O	CM	CM-8	Information System Component Inventory: The Agency develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information	Procedures: 1. Examine current inventory of information system components. Expected Results: 1. The agency develops, documents, and maintains a current inventory of the components of the information system and includes appropriate information to track components (e.g., manufacturer, model number, serial number, software license information, system/component owner).			
49	O	MA	MA-1	System Maintenance Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	Procedures: 1. Examine system maintenance policy and procedures. 2. Interview agency personnel with system maintenance responsibilities to determine how often system maintenance policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine system maintenance policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. System maintenance policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the Agency. 2. System maintenance policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when Agency review indicates updates are required. 3. System maintenance policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.			

50	O	MA	MA-2	Controlled Maintenance: The Agency schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.	Procedures: 1. Examine system maintenance schedule/records to determine if preventive and regular maintenance on the components of system is done in accordance with manufacturer or vendor specification and/or agency requirements. 2. Examine system maintenance procedures and interview personnel with system maintenance responsibility to determine procedures for removal of information system components from the facility for repair. Expected Results: 1. Routine preventative maintenance is performed regularly and in accordance with guidance from the vendor. 2. Agency officials approve the removal of the information system or information system components from the facility when repairs are necessary. All information is removed from associated media using agency approved procedures.			
51	O	MA	MA-3	Maintenance Tools: The Agency approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.	Procedures: 1. Examine maintenance tools and associated approval documentation. 2. Examine system maintenance policy. Expected Procedures: 1. All maintenance tools are approved, and include hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). 2. The agency approves, controls, and monitors the use of information system maintenance tools.			

52	O	MA	MA-4	Remote Maintenance: The Agency approves, controls, and monitors remotely executed maintenance and diagnostic activities.	Procedures: 1. Interview personnel with maintenance responsibility to determine if remote mainteance activities are performed on the system. 2. Examine remote maintenance records. 3. Examine remote maintenance session configuration settings. 4. Examine system maintenance policy and procedures. Expected Results: 1. Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). 2. The agency maintains records for all remote maintenance and diagnostic activities. 3. Remote maintenance sessions are protected with: (i) encryption and decryption of communications; (ii) strong identification and authentication techniques; and (iii) remote disconnect verification. 4. If password-based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service.			
53	O	MA	MA-5	Maintenance Personnel: The Agency allows only authorized personnel to perform maintenance on the information system	Procedures: 1. Examine procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel. Expected Results: 1. Only authorized personnel are authorized to perform maintenance on the information system. Maintenance personnel have appropriate access authorizations to the information system. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.			

54	O	SI	SI-1	System And Information Integrity Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	Procedures: 1. Examine system and information integrity policy and procedures. 2. Interview agency personnel with system and information integrity responsibilities to determine how often system and information integrity policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine system and information integrity policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. System and information integrity policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the Agency. 2. System and information integrity policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when Agency review indicates updates are required. 3. System and information integrity policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.			

55	O	SI	SI-2	Flaw Remediation: The Agency identifies, reports, and corrects information system flaws.	Procedures: 1. Examine flaw remediation policy and procedures and interview personnel with flaw remediation responsibility to determine how information system flaws are identified. 2. Examine list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws). 3. Examine test results from the installation of software to correct information system flaws. Expected Results: 1. The agency uses more than one type of vulnerability identification resource to ensure accurate and timely knowledge: -Vendor Web sites and mailing lists -Third-party Web sites -Third-party mailing lists and newsgroups (e.g., the US-CERT Cyber Security Alerts) -Vulnerability scanners -Vulnerability databases (e.g. National Vulnerability Database (NVD)) -Enterprise patch management tools (e.g., Altiris) 2. The agency installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedure or incident response. 3. The agency tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation			

56	O	SI	SI-3	Malicious Code Protection: The information system implements malicious code protection that includes a capability for automatic updates.	Procedures: 1. Examine malicious code protection mechanisms (e.g., spam/spyware and virus protection) and network design diagrams to verify the location of malicious code protection mechanisms. 2. Examine malicious code protection mechansims configuration settings. 3. Examine malicious code protection mechansims and records of malicious code protection updates to verify the capability to automatically update malicious code definitions is in use. Expected Procedures: 1. The agency employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. 2. The agency uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), and are configured to perform periodic scans of the information system as real-time scans of files from external sources. 3. The agency updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available. The most current available definition file is in use.			

57	O	SI	SI-4	Information System Monitoring Tools And Techniques: The Agency employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.	Procedures: 1. Examine information system design documentation to determine if the agency employs information system monitoring tools and techniques to 2. Examine information system design documentation to determine the location of information system monitoring tools within the network. Expected Results: 1. The system has intrusion detection capability which may include the following: intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software. 2. Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions.			

58	O	SI	SI-5	Security Alerts and Advisories: The Agency receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.	Procedures: 1. Examine procedures addressing security alerts and advisories and records of security alerts and advisories to determine how the agency receives information system security alerts and advisories. 2. Examine procedures addressing security alerts and advisories and records of security alerts and advisories to determine actions taken in response to security alerts and advisories. Expected Results: 1. Agency personnel with security alert/advisory responsibility subscribe to third-party vulnerability mailing lists and vendor mailing lists that highlight the most critical vulnerabilities (e.g., the US-CERT Cyber Security Alerts). 2. Security alerts and advisories are issued to appropriate agency personnel, who determine the significance of the threat or vulnerability; establish which systems are vulnerable or exposed; evaluate the impact on the systems, the agency and network if the vulnerability is not removed and is exploited; determine the risks involved with applying the patch or non-patch remediation; identify whether the fix will affect the functionality of other software applications or services through research and testing and make a determination on whether or not to apply a fix or not.			
59	O	SI	SI-9	Information Input Restrictions: The Agency restricts the information input to the information system to authorized personnel only.	Procedures: 1. Examine access control policy and procedures; and examine technical control SCSEM results for each technical platform within scope from the Safeguard review. Expected Results: 1. Results from the technical control SCSEMs indicate systems employ restrictions on personnel authorized to input information to the information system to include limitations based on specific operational/project responsibilities.			

60	O	SI	SI-12	Information Output Handling And Retention: The Agency handles and retains output from the information system in accordance with Agency policy and operational requirements.	Procedures: 1. Examine procedures addressing information system output handling and retention to determine how the agency handles FTI output from the information system (output includes paper and digital media). Expected Results: 1. Output from the system that includes FTI is handled in accordance with labeled or marked instructions on information system output (including paper and digital media) that includes, but not limited to, special instructions for dissemination, distribution, transport, or storage of information system output.			
61	O	IR	IR-1	Incident Response Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	Procedures: 1. Examine incident response policy and procedures. 2. Interview agency personnel with incident response responsibilities to determine how often incident response policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine incident response policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Note: The focus of the IR controls evaluation should be surrounding the FTI and not related to the entities' entire operation. Expected Results: 1. Incident response policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the Agency. 2. Incident response policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when Agency review indicates updates are required. 3. Incident response policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.			

62	O	IR	IR-2	Incident Response Training: The Agency must train personnel in their incident response roles and responsibilities with respect to the information system and Federal tax information; and provide refresher training on an annual basis.	Procedures: 1. Examine procedures addressing incident response training to determine if the agency identifies and documents personnel with significant incident response roles and responsibilities. 2. Examine incident response training records to determine the frequency of training. 3. Examine the incident response training material to determine if the material addresses the procedures and activities necessary to fulfill incident response roles and responsibilities. Expected Results: 1. The agency identifies and documents personnel with significant incident response roles and responsibilities. 2. The agency provides incident response training to personnel with incident response roles and responsibilities. Initial training is provided, and refresher training is provided at least annually. 3. The incident response training material addresses the procedures and activities necessary to fulfill the incident response roles and responsibilities.			
63	O	IR	IR-3	Incident Response Testing and Exercises: The Agency tests and/or exercises the incident response capability for the information system annually using [Assignment: Agency-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.	Procedures: 1. Examine incident response testing policy and procedures addressing incident response testing and exercises and incident response testing material to determine the tests/exercises defined by the agency. 2. Examine procedures addressing incident response testing and exercises to determine the frequency and types of test/exercises for incident response testing. 3. Examine incident response test results to verify results are documented. Expected Results: 1. The agency defines incident response tests/exercises. 2. The agency tests/exercises the incident response capability for the information system using agency-defined tests/exercises at least annually. 3. The agency documents the results of incident response tests/exercises.			

64	O	IR	IR-4	Incident Handling: The Agency implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	Procedures: 1. Examine procedures addressing incident handling capability. Expected Results: 1. Agency incident response procedures address an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery and post-incident activity.			
65	O	IR	IR-5	Incident Monitoring: The Agency tracks and documents information system security incidents on an ongoing basis.	Procedures: 1. Examine incident response records and documentation to determine the agency's incident tracking capability. Expected Results: 1. The agency tracks and documents information system security incidents on an ongoing basis.			
66	O	IR	IR-6	Incident Reporting: The Agency promptly reports incident information to appropriate authorities	Procedures: 1. Examine incident reporting records and documentation to determine if the agency promptly reports incident information to appropriate authorities. 2. Examine incident reporting records and documentation to determine if the personnel reports weaknesses and vulnerabilities in the information system to agency officials in a timely manner. Expected Results: 1. The Agency promptly reports incident information involving a compromise of FTI to the appropriate Agent-in-Charge, TIGTA. 2. In addition to incident information, weaknesses and vulnerabilities in the information system are reported to appropriate agency officials in a timely manner to prevent security incidents.			

67	O	AT	AT-1	Security Awareness and Training Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	Procedures: 1. Examine security awareness and training policy and procedures. 2. Interview agency personnel with security awareness and training responsibilities to determine how often security awareness and training policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine security awareness and training policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. Security awareness and training policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the Agency. 2. Security awareness and training policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when Agency review indicates updates are required. 3. Security awareness and training policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.			

68	O	AT	AT-2	Security Awareness: The Agency ensures that all users (including managers and senior executives) receive basic information system security awareness training consistent before authorizing access to the system, when required by system changes, and annually thereafter.	Procedures: 1. Examine security awareness and training policies, procedures and records to determine if: (i) security awareness instruction is provided to all users; (ii) records include the type of instruction received and the date completed; and (iii) initial and refresher instruction is provided at least annually. 2. Examine security awareness and training materials to determine if the materials address the requirements of the Agency. Expected Results: 1. Security awareness instruction is provided to all users; (ii) records include the type of instruction received and the date completed; and (iii) initial and refresher instruction is provided at least annually. 2. The annual IT security awareness training for Agency employees addresses the security awareness and training requirements for employees of the Agency. Security awareness training complies with C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50 by identifying employees with significant information security responsibilities for systems storing, processing or transmitting FTI, and providing role-specific training, providing annual security awareness to users of systems containing FTI, and providing refresher training on an annual basis.			

69	O	AT	AT-3	Security Training: The Agency identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system, when required by system changes, and annually thereafter.	Procedures: 1. Examine security training policies, procedures and records to determine if the Agency identifies personnel with significant information system security responsibilities and documents those roles and responsibilities. 2. Examine security training policies, procedures and records to determine if: (i) the Agency provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system; (ii) records include the type of security training received and the date completed; and (iii) provides refresher training when required by system changes and annually thereafter. 3. Examine the security training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities. 4. Obtain a copy of the document that lists personnel who have been identified as having key information system security roles and responsibilities.			
					Expected Results: 1. The Agency identifies personnel with significant information system security responsibilities and documents those roles and responsibilities. 2. The Agency provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system; records include the type of security training received and the date completed; and provides refresher training when required by system changes and annually thereafter. 3. The security training material addresses the procedures and activities necessary to fulfill those roles and responsibilities. 4. The document provides a listing of employees who have been identified as having key information system security roles and responsibilities.			

70	O	AT	AT-4	Security Training Records: The Agency documents and monitors individual information system security training activities including basic security awareness training and specific information system security training	Procedures: 1. Examine security awareness and training policy, procedures addressing security training records, security awareness and training records, and other relevant documents to determine if the Agency monitors and fully documents basic security awareness training and specific information system security training. 2. Inspect the training records of employees and verify that each has up-to-date security training records on file. 3. Examine applicable documents, to determine if the Agency documents the requirement to maintain security training records for contractors. Expected Results: 1. The Agency monitors and fully documents basic security awareness training and specific information system security training. 2. Each user has a training record that (i) identifies security training courses is taken and (ii) the record is being maintained and updated. 3. Contractors are required to complete the mandatory security training. Sample Size = 5			

71	T	IA	IA-1	Identification And Authentication Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	Procedures: 1. Examine identification and authentication policy and procedures. 2. Interview agency personnel with identification and authentication responsibilities to determine how often identification and authentication policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine identification and authentication policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. Identification and authentication policies and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the Agency. 2. Identification and authentication policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when Agency review indicates updates are required. 3. Identification and authentication policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.			

72	T	IA	IA-4	Identifier Management: The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [Assignment: organization-defined time period] of inactivity; and (vi) archiving user identifiers.	Procedures: 1. Examine a list of information system accounts for each system platform in scope for the computer security review. 2. Examine procedures addressing information system account acess authorization. 3. Examine policy and procedures addressing dorman information system accounts. 4. Examine user account archive for each system platform in scope for the computer security review. Expected Results: 1. All user identifiers are unique. 2. As part of the account authorization procedures, authorization to issue a user account to an individual from an appropriate office (e.g., manager) is received and the identify of each user is verified prior to account access being authorized. The user identifier (i.e., user ID) is issued directly to the user. 3. User IDs are disabled after 90 days of inactivity on the information system. 4. User IDs are archived.			
73	T	IA	IA-5	The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	Procedures: 1. Examine policy and procedures addressing password composition. 2. Examine procedures addressing user account management and password distribution. Expected Results: 1. Policy states passwords are required to be a minimum length of 8 characters in a combination of alpha and numeric or special characters. 2. Procedures for initial password distribution to new users, for replacing forgotten/compromised password passwords and revoking passwords are included.			

74	T	AC	AC-1	Access Control Policy And Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	Procedures: 1. Examine access control policy and procedures. 2. Interview agency personnel with access control responsibilities to determine how often access control policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine access control policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. Access control policies and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the Agency. 2. Access control policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when Agency review indicates updates are required. 3. Access control policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.			

75	T	AC	AC-18	Wireless Access Restrictions: The Agency: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system	Procedures: 1. Examine procedures addressing wireless implementation and usage (including restrictions), activities related to wireless authorization, monitoring, and control, information system audit records and other relevant documents or records to determine if the Agency: i. establishes usage restrictions and implementation guidance for wireless technologies ii. documents, monitors, and controls wireless access to the information system iii. authorizes the use of wireless technologies. 2. Examine policy and procedures addressing wireless implementation and usage (including restrictions) and other relevant documents or records to determine if the access control policy and procedures are consistent with NIST Special Publication 800-48 and address usage, implementation, monitoring, and authorization of wireless technologies. 3. Examine procedures addressing wireless implementation and usage (including restrictions), activities related to wireless authorization, monitoring, and control, information system audit records and other relevant documents or records to determine if 4. Examine procedures addressing wireless implementation and usage (including restrictions), activities related to wireless authorization, monitoring, and control, information system audit records and other relevant documents or records to determine if wireless access is only permitted through the use of authentication with encryption.			

					Expected Results: 1. A documented usage restriction and implementation guidance exist and wireless are access and controls are monitored. Additionally the Agency requires authorization before the user of wireless technologies. 2. The Agency wireless access control policies are consistent with NIST Wireless Network Security Policies by addressing encryption of communications, device authentication, physical security, replay protection, and wireless intrusion detection and prevention systems. 3. Wireless users have been authorized to access the information system. 4. Wireless access is only permitted through the use of authentication with encryption.			

76	T	AC	AC-19	Access Control for Portable and Mobile Devices: The Agency: (i) defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices; (ii) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (iii) authorizes, monitors, and controls device access to organizational information systems.	Procedures: 1. Examine access control policy, procedures addressing access control for portable and mobile devices, information system design documentation, information system audit records and other relevant documents or records to determine if the Agency: i. defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices ii. establishes and documents restrictions and implementation guidance for portable and mobile devices iii. monitors and controls the use of portable and mobile devices iv. appropriate Agency officials authorize the use of portable and mobile devices and device access to Agency information systems. 2. Interview Agency personnel with access to the information system and examine Agency documents detailing the use of portable and mobile devices to determine if personnel are complying with the usage restrictions and applying the implementation guidance on the use of portable and mobile devices in accordance with Agency policy and procedures. 3. Examine access control policy, procedures addressing access control for portable and mobile devices, information system design documentation and other relevant documents or records to determine if removable hard drives or encryption is used to protect information on portable and mobile devices. Expected Results: 1. The Agency: i. defines a mandatory suite of protective software and s iv. appropriate Agency officials authorize the use of portable and mobil 2. Agency personnel comply with portable and mobile device policies ar 3. Information on portable devices is protected using cryptography.			

77	T	AC	AC-20	Use of External Information Systems: The Agency establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit Agency-controlled information using an external information system.	Procedures: 1. Examine access control policy, procedures addressing the use of external information systems, external information systems terms and conditions, list of types of applications accessible from external information systems, maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems, information system configuration settings and associated to determine if the use of a personally owned information system meets the following minimum requirements as defined by the access control policy and procedures regarding: (i) the types of applications that can be accessed from personally owned information systems; (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (iii) how other users of the personally owned information system will be prevented from accessing federal information; (iv) the use of virtual private networking (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of malicious code protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, malicious code definitions, firewall version updates, malicious code protection definitions). Expected Results: 1. The use of personally-owned information systems to access Agency information systems is not allowed.			

78	T	AU	AU-1	Audit And Accountability Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	Procedures: 1. Examine audit and accountability policy and procedures. 2. Interview agency personnel with audit and accountability responsibilities to determine how often audit and accountability policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine audit and accountability policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. Audit and accountability policies and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the Agency. 2. Audit and accountability policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when Agency review indicates updates are required. 3. Audit and accountability policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.			
79	T	AU	AU-7	Audit Reduction and Report Generation: The information system provides an audit reduction and report generation capability.	Procedures: 1. Interview personnel with system audit monitoring responsibility to determine if a capability for audit reduction and report generation is implemented. 2. Examine the audit reduction and report generation tool used, as well as a sample audit report. Expected Results: 1. Audit reduction and report generation capability is provided either by the system itself, or by a third party software tool. 2. Examiniation of the tool and report indicates the tool is functioning properly.			

80	T	AU	AU-11	Audit Record Retention: The organization retains audit records for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Procedures: 1. Examine procedures addressing audit record retention. 2. Examine system audit records to verify the retention period. Expected Results: 1. The proedures define the retention period for audit records generated by the information system. 2. The agency retains information system audit records for the agency-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.			
81	T	SC	SC-1	System And Communications Protection Policy And Procedures: The Agency develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	Procedures: 1. Examine system and communications protection policy and procedures. 2. Interview agency personnel with system and communications protection responsibilities to determine how often system and communications protection policy and procedures (i) are reviewed by responsible parties within the agency; and (ii) are updated, when agency review indicates updates are required. 3. Examine system and communications protection policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance. Expected Results: 1. System and communications protection policies and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the Agency. 2. System and communications protection policy and procedures (i) are periodically reviewed by responsible parties within the agency; and (ii) are updated, when Agency review indicates updates are required. 3. System and communications protection policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.			

82	T	SC	SC-7	Boundary Protection: The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.	Procedures: 1. Examine system and communications protection policy, procedures addressing boundary protection, information system design documentation, boundary protection hardware and software, information system architecture and configuration documentation, information system configuration settings and associated documentation, and other relevant documents or records to determine if the: (i) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. (ii) the Agency physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces. (iii) the Agency prevents public access into the organization's internal networks except as appropriately mediated. (iv) the Agency limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic. (v) the Agency defines the security controls (i.e., boundary protection devices and architectural configuration of the devices) appropriate at eac interface to a telecommunication service and mplements a mana with any external telecommunication service, implementing contr appropriate to the required protection of the confidentiality and in information being transmitted. (vi) the information system denies network traffic by default and network traffic by exception.			

83	T	SC	SC-8 SC-9 PB1075 5.17.6.2	Transmitting FTI - All FTI must be protected when transmitted across a WAN or within a LAN.	Procedures: 1. Examine network design diagram and interview agency personnel to determine if FTI is encrypted when transmitted across a Wide Area Network (WAN). 2. Examine network design diagram and interview agency personnel to determine if FTI is encrypted when transmitted across the Local Area Network (LAN). 3. If encryption is not used, interview agency personnel to determine how FTI is protected while in transit over the LAN and WAN. Expected Results: 1. Transmissions are encrypted using a key no less than 128 bits in length, or FIPS 140-2 compliant, whichever is stronger. All transmissions of FTI between the agency and IRS are executed using the Tumbleweed solution. 2. Transmissions are encrypted using a key no less than 128 bits in length, or FIPS 140-2 compliant, whichever is stronger. 3. If encryption is not used to transmit data over the WAN, unencrypted cable circuits of copper or fiber optics is an acceptable means of transmitting FTI. If encryption is not used to transmit data over the LAN, the agency must use other compensating mechanisms (e.g., switched vLAN technolog optic medium, etc.)			
84	T	SC	SC-8 SC-9 PB1075 5.17.6.2	Transmitting FTI - All FTI must be protected when transmitted across a WAN or within a LAN.	Procedures: 1. If dedicated circuits are used in place of encryption for transmission of FTI across the WAN, interview agency personnel to determine what measures are in place to protect the circuits. Expected Results: 1. Circuits are maintained on cable and not converted to unencrypted radio (microwave) transmission. The cable is protected by either being buried underground, or run through plenum area in walls, ceilings or floors. Access to cable and switching rooms is restricted. All wiring, conduits, and cabling are within the control of agency personnel and that access to routers and network monitors are strictly controlled.			

85	T	SC	SC-12	Cryptographic Key Establishment and Management: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures	Procedures: 1. Examine system and communications protection policy, procedures addressing cryptographic key management and establishment, information system design documentation; information system configuration settings and associated documentation and other relevant documents or records. (including developer design documentation) to determine if the information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and management and how the mechanisms and procedures are implemented. Expected Results: 1. The information system utilizes automated mechanisms with supporting procedures in place for digital certificate generation, installation, and distribution. Subscriber key pairs are generated and stored using FIPS 140-2 Security Level 2 or higher cryptographic modules. The same public/private key pair is not be used for both encryption and digital signature. Private keys are protected using, at a minimum, a strong password. A certificate is revoked if the associated private key is compromised; management requests revocation; or the certificate is no longer needed.			
86	T	SC	SC-15	Collaborative Computing: The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.	Procedures: 1. Examine the information system to verify whether or not it has collaborative computing mechanims (Collaborative computing mechanisms include, for example, video and audio conferencing capabilities.). If the system does have collaborative computing mechanisms, then verify the ability to remotely execute those capabilities. Expected Results: 1. The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.			

87	T	SC	SC-17	Public Key Infrastructure Certificates: The Agency issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider	Procedures: 1. Examine system and communications protection policy, procedures addressing public key infrastructure certificates, public key certificate policy or policies, public key issuing process, and other relevant documents or records to determine if the Agency develops and implements a certificate policy and certification practice statement for the issuance of public key certificates at the Agency-wide level. Expected Results: 1. The Agency develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used at the Agency-wide level.			
88	T	SC	SC-18	Mobile Code: The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of mobile code within the information system.	Procedures: 1. Examine system and communications protection policy, procedures addressing mobile code, mobile code usage restrictions, mobile code implementation guidance, and other relevant documents or records to determine if the Agency: i. establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously ii. documents, monitors, and controls the use of mobile code within the information system iii. requires Agency officials to approve the use of mobile code. Expected Results: 1. The Agency establishes usage restrictions and implementation guidance for mobile code technologies. Mobile code usage requires authorization and are documented and monitored. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript.			

89	T	SC	SC-19	Voice Over Internet Protocol: The Agency: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of VoIP within the information system.	Procedures: 1. Examine applicable system and communications protection policy, procedures addressing VoIP, VoIP usage restrictions, and other relevant documents or records to determine if the Agency has established policies and guidance for the use of VoIP. Expected Results: 1. The Agency: (i) establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously, (ii) documents, monitors, and controls the use of VoIP within the information system, (iii) requires Agency officials to approve the use of VoIP.			
90	NA	NA	PB1075 5.17.6.5	Electronic Mail - FTI shall not be transmitted or used on E-mail systems.	Procedures: 1. Examine agency policy for handling FTI and interview agency personnel to determine if FTI is transmitted via email. 2. If FTI must be transmitted via email, examine agency policy and interview agency personnel to determine what measures are in place to secure FTI during email transmission. Expected Results: 1. Agency policy states FTI shall not be transmitted or used on email systems. 2. If it is necessary to transmit FTI via email, the following precautions must be taken to protect FTI sent via email: • FTI is encrypted in the email • Attachments containing FTI are encrypted • Ensure that all messages sent are to the proper address, and • Employees should log off the computer when away from the area.			

91	NA	NA	PB1075 5.17.6.6	Fax Machines - FTI fax transmissions are properly secured.	Procedures: 1. Examine agency policy for handling FTI and interview agency personnel to determine if FTI is transmitted via Fax machine. Expected Results: 1. If FAX machines are used to transmit FTI the following security mechanisms are in place to protect Fax transmissions: • A trusted staff member is located at both the sending and receiving fax machines. • Broadcast lists and other preset numbers of frequent recipients of FTI are maintained and periodically updated • Fax machines are placed in a secured area. • A cover sheet is included on fax transmissions that explicitly provides guidance to the recipient, which includes: - A notification of the sensitivity of the data and the need for protection - A notice to unintended recipients to telephone the sender—collect if necessary—to report the disclosure and confirm destruction of the information.			

IRS Safeguard SCSEM Legend

Test Case Tab: Execute the test cases and document the results to complete the IRS Safeguard Computer Security review. Reviewer is required to complete the following columns: Actual Results, Comments/Supporting Evidence. Please find more details of each column below.

ID		**Identification number of SCSEM test case**
PUB 1075	**Control Class**	NIST 800-53/PUB 1075 Control Class (Management, Operational, Technical)
	Control Family	NIST 800-53/PUB 1075 Control Family (Risk Assessment, Security Planning, System and Services Acquisition, Security Assessment, Personnel Security, Contingency Planning, Configuration Management, System Maintenance, System and Information Integrity, Incident Response, Security Awareness and Training, Identification and Authentication, Access Control, Audit and Accountability, System and Communications Protection)
	REF. ID	NIST 800-53/PUB 1075 Reference Identification (1, 2, etc.)
Control Objective		Objective of test procedure.
Test Procedure & Expected Results		Detailed test procedures to follow for test execution, and the expected outcome of the test step execution that would result in a Pass.
Actual Results		The actual outcome of the test step execution, i.e., the actual configuration setting observed.
Pass/Fail		Reviewer to indicate if the test case pass, failed or is not applicable.
Comments / Supporting Evidence		Reviewer to include any supporting evidence to confirm if the test case passed., failed on not applicable As evidence, provide the following information for the following assessment methods: 1. Interview - Name and title of the person providing information. Also provide the date when the information is provided. 2. Examination - Provide the name, title, and date of the document referenced as the evidence. Also provide section number where the pertinent information is resident within the document (if possible). Ensure all supporting evidence to verify the test case passed or failed. If the control is marked as NA, then provide appropriate justification as to why the control is considered NA.